ABSTRACT

Army ground vehicles are equipped with electronic devices (e.g. sensors, displays, processors, weapons etc) to carry out battle missions. A standard interoperable in –vehicle network architecture is required to make onboard electronic devices more efficient, interoperable, and scalable.

This report focus on the following topics

- High level “Common Bus In-Vehicle Network Architecture” proposal for army ground vehicles to integrate and expand on-board electronic devices.
- Network protocol and topology selection, and analysis criteria.
- Service oriented architecture compliant software components or modules.
- Compliance with military standards.

Additional details are found under the background section.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
10 DEC 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	
A Common Bus In-Vehicle Network Architecture For Ground Army Vehicles	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Macam S Dattathreya	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **US Army RDECOM-TARDEC 6501 E 11 Mile Rd Warren, MI 48397-5000, USA**	8. PERFORMING ORGANIZATION REPORT NUMBER **20439RC**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) **TACOM/TARDEC**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) **20439RC**

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT
Army ground vehicles are equipped with electronic devices (e.g. sensors, displays, processors, weapons etc) to carry out battle missions. A standard interoperable in ¡V vehicle network architecture is required to make onboard electronic devices more efficient, interoperable, and scalable. This report focus on the following topics h High level ¡§Common Bus In-Vehicle Network Architecture¡¨ proposal for army ground vehicles to integrate and expand on-board electronic devices. h Network protocol and topology selection, and analysis criteria. h Service oriented architecture compliant software components or modules. h Compliance with military standards. Additional details are found under the background section.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**41**	

Table of Contents

Table of Figures

Table of Tables

1 INTRODUCTION

1.1 Background

In general, for faster procurement, electronic devices in army vehicles are built using a kit/appliqué approach i.e. devices are attached to a vehicle on demand. This approach saves money and time but has interoperability, performance, and scalability concerns. Currently there are no commercial open network architectures in the market to address these issues. Open standard network architecture is required to minimize technology risk and to improve vehicle performance & interoperability.

This report discusses the following topics

- Network protocol and topology selection, and analysis criteria using standard network protocols & topologies.
- Military and technology standards compliance.
- Maintainability, scalability, and interoperability improvements.
- Information Assurance (Security, classification).
- Open standard, secure, high level common bus in-vehicle network architecture proposal with reduced single point network failures.
- Improved vehicle interior and power consumption.

1.2 Scope

The information described in this report is limited to the list below.

- Figure 1 Use Case for In-Vehicle Network Architecture scope.
- Figure 2 In-Vehicle Network Architecture Overview elements.
- High-level architecture concepts and approaches with no low level implementation details (this will be a topic for future work or for a new project)

- No acquisition issues are addressed (procurement cost and funding).

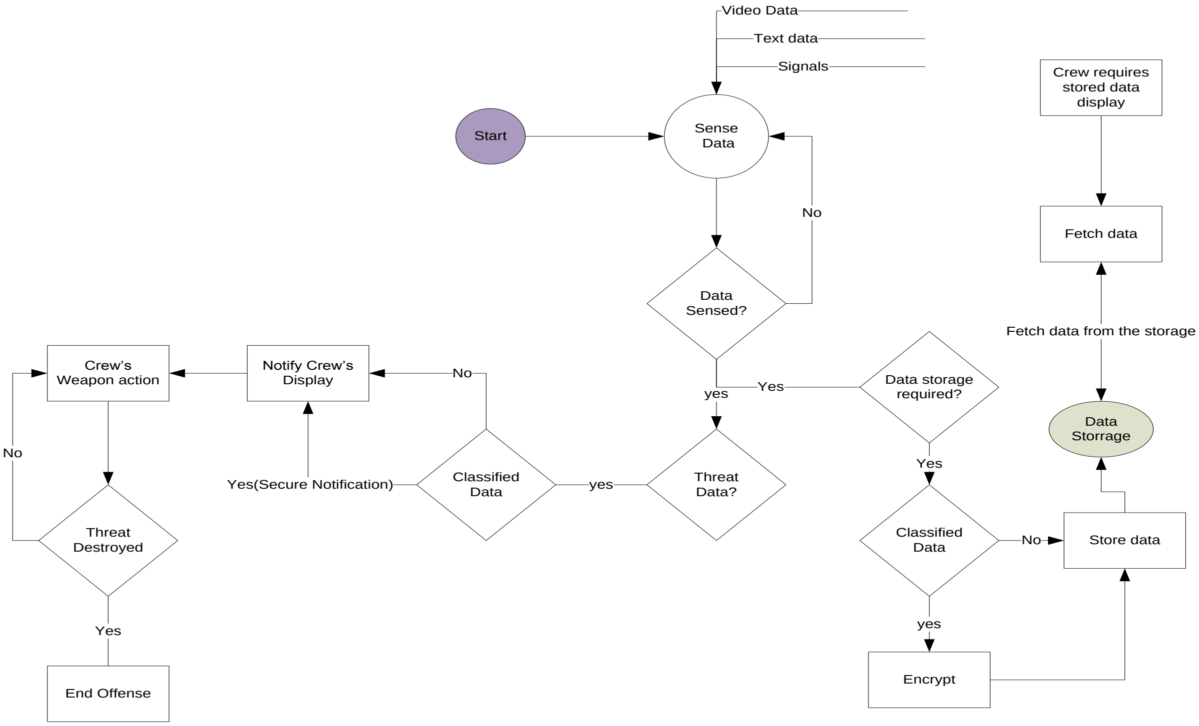

Figure 1 Use Case for In-Vehicle Network Architecture scope

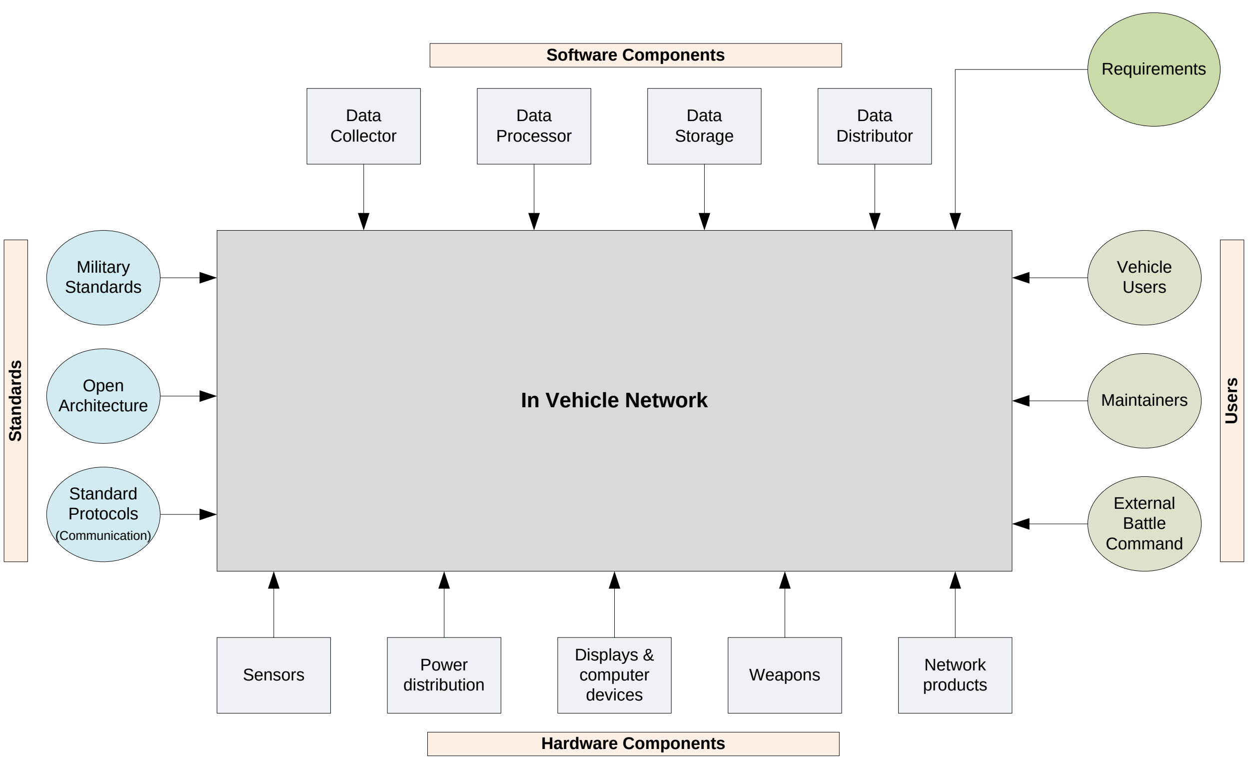

Figure 2 In-Vehicle Network Architecture Overview

2 LITERATURE SEARCH

In general, army vehicles deal with three types of data i.e. video, text and signals. To promote safe and secure transfer of these data types, appropriate network protocol and topology needs to be selected. To minimize reinvention, a literature research is conducted to gain open standard technical data from the locations listed in the REFERENCES section of this report. The study results are summarized in the sections 2.1 through 2.4. The data from this section is used for the proposed in-vehicle network architecture. The 3.4 Analysis section discusses the selection rationale.

2.1 Network protocols or specifications

This section describes the suitable network protocols and specifications used to work with army vehicle data. Each protocol discussion in this section focuses on its commercial availability, hardware obsolescence, extensibility, technical risk and open standard. Due to some internal restrictions, time triggered protocols such as time triggered CAN, time triggered Ethernet and FlexRay are not considered here.

2.1.1 Controller Area Network (CAN)

Controller Area Network (CAN) is a typical automotive bus communications standard to connect sensors, actuators and control devices without a host computer. In a CAN network multiple devices cannot send simultaneous messages and are bound to the priority based transmission.

CAN Network contentions are resolved using a bitwise arbitration and "Non Return to Zero" (NRZ) coding with bit stuffing used for messaging. Each node in a CAN network has its own clock, and no clock is sent during data transmission. Synchronization is done by dividing each bit of the frame into a number of segments: Synchronization, Propagation, Phase 1 and Phase 2.

Each CAN network node consists of a host processor, a controller and a transceiver. A CAN network consists of the following layers: application layer, object layer, transfer layer and physical layer. Per SAE J2284, for the Dual Wire physical layer, the highest bit rate for automotive use is typically 500 kb/s. But per ISO11898 the maximum bit rate is1 Mb/s.

CAN hardware is commercially available since 1991. It is less susceptible to hardware obsolescence, has minimum technology risk and is easy to extend to additional devices.

2.1.2 Gigabit Ethernet (802.3ab)

Gigabit Ethernet (IEEE 802.3ab or 1000BASE-T) transmits Ethernet frames at a rate of a gigabit per second. The gigabit Ethernet can be used to connect any electronic devices with

Ethernet ports. In an Ethernet network, multiple devices can send simultaneous messages but are limited to the carrier's or cable's bandwidth.

To transmit data over four twisted pairs in CAT 5 cable, this protocol uses an encoding scheme to keep the lowest possible symbol rate. The network segment has 100m maximum length restriction for this. It must utilize CAT 5 cable at minimum. This protocol uses multilevel amplitude signaling using five level encoding systems i.e. PAN-5. In an Ethernet, to encode 8 bits, 2^8 or 256 symbols are required since there are 256 possible pattern combinations

Gigabit Ethernet hardware is commercially available since 1991 and is less susceptible to hardware obsolescence and has minimum technology risk and is easy to extend to additional devices.

2.1.3 USB 2.0

Universal Serial Bus (USB) transmits data at 480 Mbit/s by toggling the data lines between the J state and the opposite K state. The USB can be used to connect electronic devices to a computer or another device with USB port. A USB system has an asymmetric design, consisting of a host, a multitude of downstream USB ports, and multiple peripheral devices connected in a tiered-star topology.

USB encodes data using the Non return to zero, inverted (NRZI) convention; a 0 bit is transmitted by toggling the data lines from J to K or vice-versa, while a 1 bit is transmitted by leaving the data lines as-is. To ensure a minimum density of signal transitions, USB uses bit stuffing; an extra 0 bit is inserted into the data stream after any appearance of six consecutive 1 bits.

USB hardware is commercially available since 2000. It is less susceptible to hardware obsolescence and has minimum technology risk but extending to additional devices require USB hubs.

2.1.4 IEEE 1394

The IEEE 1394 is a serial bus standard for high-speed communications and isochronous[1] real-time data transfer. These are frequently used by the personal computers, as well as in digital video, automotive, and aeronautics applications. IEEE 1394 supports multiple hosts per bus, and is designed to support Plug and play and hot swapping. IEEE 1393b supports transfer rates of 100, 200, 400, 800, 1600 and 3200 Mbps on shielded twisted pair

[1] Isochronous transfers on the 1394 bus guarantee timely delivery of data. Each 125µs timeslot on the bus is called a frame. Isochronous transfers, unlike asynchronous transfers, do not in any way guarantee the integrity of data through a transfer. No response packet is sent for an isochronous transfer. Isochronous transfers are useful for situations that require a constant data rate but not necessarily data integrity, such as audio or video streaming.

All data is sent along the IEEE 1394 bus in serial four byte (32-bit) words, called *quadlets*. These *quadlets* are encoded together with their clock signals onto Non Return to Zero (NRZ) bus signals, using a technique known as Data-Strobe (DS) coding. This improves transmission reliability by ensuring that only one of the two signals changes in each data bit period.

IEEE 1394's most common implementation is 2 twisted pairs of copper cabling. The copper cable it uses can be up to 4.5 meters (15 ft) long. In its six-circuit or nine-circuit variations, it can supply up to 45 watts of power per port at up to 30 volts, allowing moderate-consumption devices to operate without a separate power supply.

IEEE 1394 hardware is commercially available since 2003. It is less susceptible to hardware obsolescence and has minimum technology risk and extending to additional devices is not an option as it is a serial bus.

2.1.5 Digital Visual Interface (DVI)

The Digital Visual Interface (DVI) is a high visual quality standard to connect a computer and a display device. The DVI uses a digital protocol to transmit desired illumination of pixels as binary data. The DVI interface is independent of display technology and a single connector supports both analog and digital signals. DVI uses Transition Minimized Differential Signaling TDMS technology for transmitting high-speed serial data.

TMDS uses differential signaling to reduce electromagnetic interference (EMI) to increase accuracy and faster signal transfers. DVI supports 150 Mpixel/sec data transfers over a three twisted pair TMDS DVI link where each of the links corresponds to a different RGB component.

With a single DVI link, the largest resolution possible at 60 Hz is 2.75 megapixels with a maximum screen resolution at 60 Hz of 1915 x 1436 pixels (standard 4:3 ratio), 1854 x 1483 pixels (5:4 ratio) or 2098 x 1311 (widescreen 8:5 ratio).

DVI hardware is commercially available since 1999. It is less susceptible to hardware obsolescence and has minimum technology risk and extending additional devices is not an option as it is a serial bus.

2.2 Network topologies

Electronic devices must be interconnected to obtain maximum efficiency and accuracy with reduced latencies & cabling. The devices layout requires a single standard or hybrid of multiple topologies to minimize the vehicle restrictions and maximize vehicle performance. A topology allows devices for data exchange and resource sharing. This section describes several topologies focusing on its layout, operation, pros and cons to assist appropriate topology selection.

2.2.1 Bus topology

Layout

All the devices in this topology are connected to a common shared backbone bus (cable) as shown in the Figure 3 Buss topology.

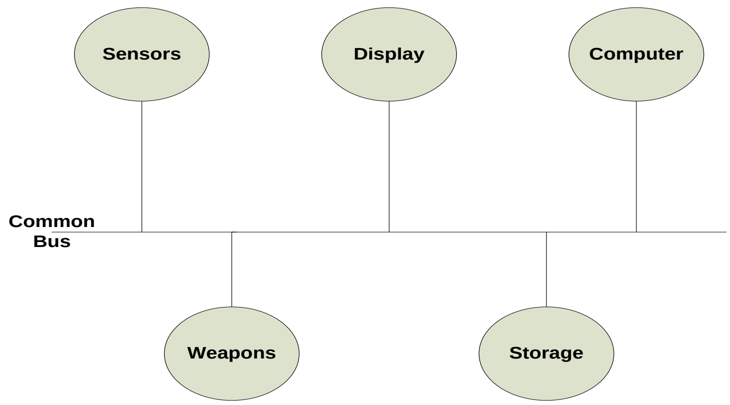

Figure 3 Buss topology

Operation

In a bus network of Sensors, Display, Computer, Weapons and Storage devices, source device ‘Sensors’ sends a request/process message on the network to a target device ‘Computer’. All the devices in this bus topology will read the message and only ‘Computer’ will accept it and then process it. No central unit or device is used

Pros

- Simple and economical implementation, straightforward expansion of devices with less cabling (less weight).
- Each device on the network can broadcast messages at the same time with equal priority.
- No host or a central computer to manage resources as each device manages its own.
- Best suited for smaller networks.

Cons

- Cable length is limited and a single cable breakage ends the entire network with difficult problems determination.
- Due to shared bandwidth, the devices suffer performance degradation when more devices are added to the network.
- Must have closed loops with proper termination points.
- Not a good topology for larger network of devices.

2.2.2 Ring topology

Layout

All the devices in this topology are connected so that every device has only two other connecting devices as shown in the Figure 4 Ring topology.

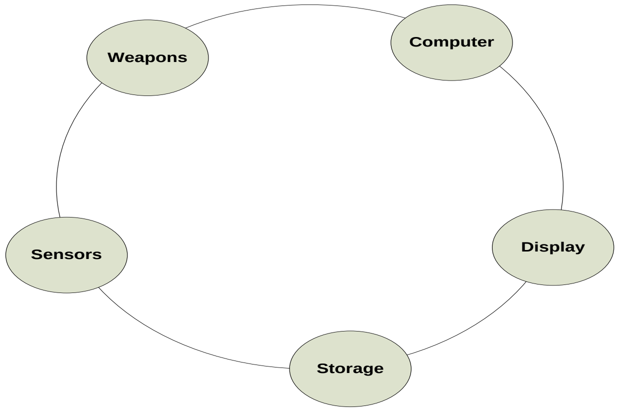

Figure 4 Ring topology

Operation

In a ring network of Sensors, Display, Computer, Weapons and Storage devices, source device 'Sensor' sends a request/process message on the network to a target device 'Computer'. The message travels from 'Sensors' to 'Computer' passing through 'Weapons'. The 'Weapons' handle this message and passes to 'Computer' where it accepts the message and process it. No central unit/network devices such as servers are used.

Pros

- Each device on the network can broadcast messages at the same time with equal priority.
- No central server is required to manage resources as each device manages its own.
- Larger networks can be created as it works better than star topology during heavy network load.
- Provides reliable communication with less cabling.

Cons

- A break in a link or device ends the loop and the entire network is down.
- Adding, moving or changing devices on the network affects the network performance or operation.
- Difficult troubleshooting.

2.2.3 Star topology

Layout

All the devices in this topology are connected to a central device called 'Hub' as shown in the Figure 5 Star topology.

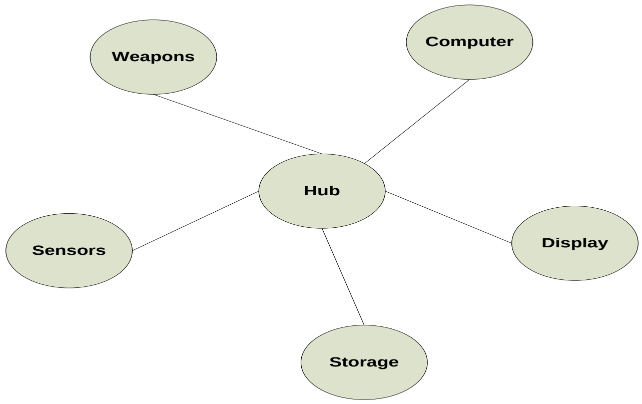

Figure 5 Star topology

Operation

In a star network of Sensors, Display, Computer, Weapons and Storage devices, source device ‘Sensor’ sends a request/process message on the network to a target device ‘Computer’. The message travels from ‘Sensors’ to ‘Computer’ passing through ‘Hub’. The ‘Hub’ handles this message and passes to ‘Computer’ where it accepts the message and processes it.

Pros

- Adding, moving or changing devices on the network with no network performance or operation impacts.
- Single device failure does not impact the network operation/performance and request messages do not pass through multiple devices before reaching the target.
- Each device is isolated by the link that connects it to the central hub.
- Multiple cable types can be used within a network.

Cons

- A break in the central hub ends the loop and the entire network is down.
- Requires a central hub device to switch data from device A to B.
- The hub limits the network size and the performance, as the entire network is limited to the hub’s throughput.

2.2.4 Mesh topology

Layout

All the devices in this topology are connected to each other through hops. Some are single and some are connected with multiple hops as shown in the Figure 6 Mesh topology.

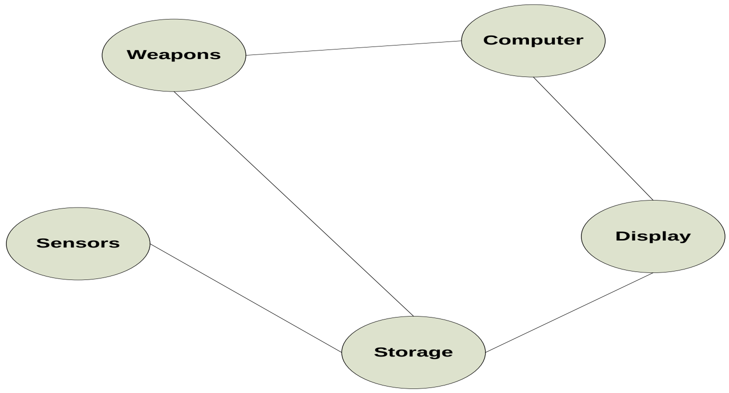

Figure 6 Mesh topology

Operation

In a Mesh network of Sensors, Display, Computer, Weapons and Storage devices, the source device 'Computer' sends a request/process message on the network to a target device 'Storage'. The message travels from 'Computer' to 'storage' hopping through 'Display' or 'Weapons' node/device. The 'Storage' accepts the message and processes it.

Pros

- Easy to troubleshoot and the network is fault tolerant.
- Single device failure does not impact the network operation/performance.
- Provides reliable communication.

Cons

- High implementation cost due to high complexity and more cabling.
- High maintenance cost due to redundant links.
- Complicated installation and reconfiguration.

2.2.5 Hierarchical topology (tree)

Layout

All the devices are connected to each other as shown in the Figure 7 Hierarchical topology (tree). Each level is connected to the next higher level in a symmetrical pattern and there will be at least three levels of hierarchy and they all work based on the root node/device.

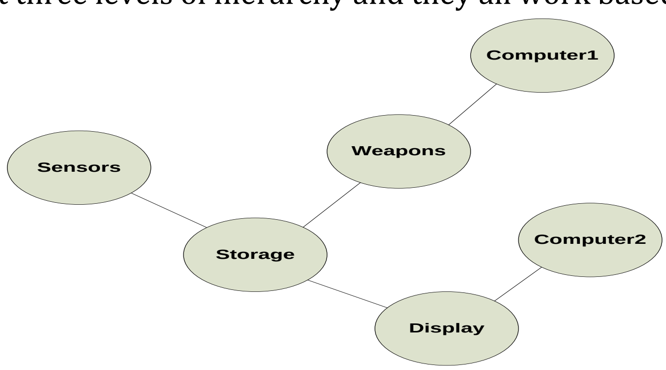

Figure 7 Hierarchical topology (tree)

Operation
In a Hierarchical network of Sensors, Display, Computer1, Computer2, Weapons and Storage devices, source device 'Computer1' sends a request/process message on the network to a target device 'Storage'. The message travels from 'Computer1' to 'storage' hopping through ''Weapons' node/device. 'Storage' accepts the message and processes it.
Pros

- Easy to troubleshoot and the network is fault tolerant.
- Single device failure does not impact the network operation/performance.
- Provides reliable communication.

Cons

- Cabling type limits the length of each segment.
- If the backbone line fails, the entire segment is failed.
- Complicated reconfiguration.

2.3 Network concepts

Networking is a process of linking multiple computing devices to share data and communicate with each other. A network consists of processing hardware and software. A network may be wide area (connecting multiple geographical locations) or it can be a peer to peer or within a geographic area such as inside a building or a vehicle.

Both wired and wireless technologies share the same or similar networking protocols [refer 2.1 Network protocols or specifications for more details]. Each device in a network has its own specific address. The information assurance requirements limit the use of wireless technology in the army ground vehicles. This section describes the various wired network technologies and its concepts.

2.3.1 Packet switching

Packet switching is an approach used by the network protocols to transmit data across a connection. The transmitted data is packaged in special format packets. The data is routed between source and destination using network devices. The packet will have the recipient address to enable network devices to transmit appropriately. Packet switching optimizes network bandwidth and minimizes transmission latency with robust communication. The current packet switching protocols are Frame relay, IP and X.25.

2.3.2 Network bandwidth & latency

Network bandwidth or throughput is the capacity of a connection between devices. The bandwidth is measured in terms of bits/second (bps). Latency is a delay in the processing of network data.

2.3.3 Network routing

In a network, routing is a process of directing the data path to an address specific device i.e. in packet switching; the routing directs the packets between the source and the destination.

2.3.4 Network operating system and networking model

A network operating system is a functional support for devices to serve requests from other devices and access other resources in the network. The Open systems Interconnection (OSI) reference model suggests network data communication architecture. The model has seven layers as shown below.

1. Physical layer: A connection between the devices and the network.
2. Data link layer: To represent data transfer method. This has two sub layers, Media Access Control (MAC) to coordinate data transmission between devices and Logical Link Control (LAC) to main the links between the devices using Service Access points (SAP).
3. Network layer: Routes messages with the best path available considering message priority, status and data congestion.
4. Transport layer: To sequence and error free transmission and to recombine fragmented packets.
5. Session layer: To determine session transactions.
6. Presentation layer: To translate data to device specific format including compression and the data direction.
7. Application layer: To interact with the network from the user community.

2.3.5 Network firewall (security)

A network firewall is a device or software, or a combination of both to prevent unauthorized network access. In a network, the firewalls are configured to permit, deny, encrypt, decrypt, or proxy data traffic between different security domains per predefined rules. The typical firewall techniques fall into packet filter, application gateway, circuit level gateway, and proxy server. In addition to network firewalls, the software based program specific access authorizations are also required to restrict unauthorized use of on board applications.

2.3.6 Network gateway

A network gateway is a system to interconnect different base protocols. A gateway can be software, hardware or a combination of both. Network gateways, depending on its supported protocols, operate at any OSI model levels.

2.3.7 Hop
In a network, hop represents the number of devices/stops the data goes through prior to reaching its destination. Larger the hop count greater the network latency.

2.3.8 IP Address
In a network, IP address is the logical address of a given device connected to the network. In local area network, the address is private. IPv4 standard addresses consist of four bytes (32 bits). Each byte of an IP address is known as an Octet. Octets can take any value between 0 and 255. Various conventions exist for the numbering and use of IP addresses.

2.3.9 Quality of service (QoS)
QoS is a broad collection of networking technologies and techniques to guarantee the predictable results from the network. The scope of QoS includes availability, throughput, delay, and error rate. QoS prioritizes the network traffic.

2.3.10 Protocol converter
To achieve interoperability, if a device has one protocol, it has to be converted to another protocol to suit the target device. The protocol converter device performs this function and influences common bus architecture in a network. The protocol converter has an internal master control protocol, slave devices and databases. The reporting commands or events have various report handling schemes. The physical media are different for RS232, RS485, and Ethernet etc.

2.4 Network architecture products
This section describes the commercially available products used in networks to minimize the production cost, testing efforts, technology risk, and logistics footprint.

2.4.1 Network router
The network routers connect two or more logical network subnets and perform data routing from one network to another network. Routers operate in controlling and forwarding plane at the OSI network layer. Current commercial routers connect multiple networks to perform multiple functions in addition to routing. Routers route messages transmitted only by a routable protocol such as IP or IPX. Ethernet, USB and FireWire (IEEE 1394) hubs are available commercially.

2.4.2 Network switch
The network switches connect two or more devices in a network and perform data switching from one device to another device. Switches operate at the OSI data link layer. The switches inspect the data packets and determine the source and destination for them and forward to the appropriate device. The network switch conserves bandwidth and provides better performance than the network hub. The switches provide four to eight

connections and multiple switches can be connected to each other to allow more devices to the network. Ethernet, USB and FireWire (IEEE 1394) hubs are available commercially.

2.4.3 Network repeater

A network repeater amplifies data signals in a network before sending on the wire. They counter the wire signal decay. If several repeaters are used in a network using a router, the devices communicating with an intermediate network have low performance when compared to devices communicating directly with the router.

2.4.4 Network hub

A network hub is a device which connects multiple devices together to form a single network segment. Hubs operate at the OSI physical model and are used as a multiport repeater. The hubs are now replaced by network switches. A hub receives incoming packets, amplifies the signal, and broadcasts it to all devices on the network including the source of that packet. Ethernet, USB and FireWire (IEEE 1394) hubs are available commercially.

2.4.5 Network firewall

A network firewall device provides restricted or protected access to the network. The network firewalls may be hardware or software or a combination of both. Many commercial routers have a built in network firewall. The Network firewall device can be configured to permit, deny, encrypt, decrypt, or proxy all network traffic between different security domains based on predefined rules and other criteria. Many commercial firewalls are currently available.

3 ARCHITECTURE DEVELOPMENT

3.1 Requirements

Army vehicle networking architecture must consider the following high level requirements;

- Capable of handling classified and unclassified information with no data contamination.
- Tolerable to individual device failures and no single point network failure.
- Lowest implementation cost with less maintenance time.
- Interoperable and meets all the information assurance and open architecture requirements.
- Compliant with military standards.
- Easy expansion of additional devices.

3.2 Concepts

This section describes the concepts introduced in the Figure 2 In-Vehicle Network Architecture Overview. The proposed architecture section provides context specific information.

3.2.1 Users

Typical users of an army vehicle are Soldiers (crew), maintenance personnel, and off vehicle commanders. Soldiers operate onboard devices during battle missions. Maintenance personnel perform routine maintenance. Off vehicle commanders communicate with the vehicle crew to carry out battle missions.

3.2.2 Software components

The data collectors, data processors, data storage and data distributors are the high level software building blocks for the proposed architecture. The data collectors receive data from various sensors and other devices. The data processors process the data per request or automatic to meet a specific functionality. The data storages assist in storing the data to a specific location to meet a specific function. The data distributors distribute data to various devices on demand or automatic. All these components are distributed and are designed for redundancy to improve availability.

3.2.3 Hardware components

The army vehicles have multiple hardware components as described in the Figure 2 In-Vehicle Network Architecture Overview. The sensors are used to gather and sense various awareness data and feed to the appropriate devices for data collection and processing. The power distribution equipment is used to supply power to the various devices. The crew members require display devices to view and analyze battle conditions, and to take actions. The computers are needed to process data and distribute it to meet mission needs. The weapons are to handle hostile mission conditions. The network products are the devices in a vehicle network to allow data configuration, communication and distribution.

3.2.4 Standards

Various military standards are required for a vehicle network. The section 3.3 Standards and compliance describes the details. The standards are required to meet the open standard and architecture requirements for army vehicles.

3.2.5 Requirements

Every network design has to meet certain requirements to fulfill the needs of an army mission. The section 3.1 Requirements describes the requirements that needs to be fulfilled to accomplish the proposed in vehicle architecture.

3.3 Standards and compliance

The proposed architecture must be compliant with the military standards described below. The proposed architecture section will evaluate and choose the applicable standards.

3.3.1 Trusted Computer System Evaluation Criteria (TCSEC)

The TCSEC is a US Department of Defense (DoD) standard for setting requirements to evaluate, classify and select computer systems to process, store and retrieve sensitive or classified data. The TCSEC is also known as the Orange Book. This standard demands the following:

- Implementation of mandatory or discretionary security policies. The user must be made accountable through identification, authentication and auditing.
- Must provide operational assurance, life cycle assurance and continuous protection assurance.

3.3.2 Multiple Independent Levels of Security (MILS)

This is a new approach to build secure systems in contrast to the DoD Orange Book. The MILS architecture was to resolve high assurance systems certification difficulty by separating out the security mechanisms and concerns into manageable components. A MILS system isolates processes into partitions. To support these partitions, the MILS architecture is divided into three layers; separation kernel, middleware services and applications. MILS architecture reduces the security functionality into four security policies i.e. information flow, data isolation, periods processing and damage limitation.

3.3.3 Department of defense architecture framework (DODAF)

The DoDAF v1.5 provides guidance for architects to begin representing net-centric architectural constructs. Net-centricity is an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. The following is the guidance list.

- Populate and utilize the net-centric environment
- Accommodate the unanticipated user
- Promote the use of communities of interest and support shared infrastructure

3.3.4 Information assurance Implementation (Document# DOD 8500.2)

The DoD Information Assurance Certification and Accreditation Process (DIACAP) is the DoD process to ensure the risk management application on information systems. The DIACAP defines the information assurance controls implementation in the DOD D8500.2. The IA controls are determined based on the system's mission assurance category (MAC) and confidentiality level (CL). The current requirement is to use MAC II category and the secret confidentiality level.

3.4 Analysis

The army ground vehicle network architecture design is complex and challenging due the following contributing factors:

- 100% uptime with very minimum single point network failures.
- Minimum clutter and restricted cabling.
- Soldier's life or safety is the superseding factor for any trade off space.
- Minimum latency requirements.
- Economical with reduced logistics footprint.
- Longer mean time between failures with minimum failures (especially in a mission).

This section describes the protocol technology selection methodology, topology selection process, bandwidth analysis, other network devices selection, and analysis of alternative architectures to meet the requirements of common bus network architecture.

3.4.1 Protocol Selection methodology

The items listed under Table 1 Technology Selection Factors with weights are the focus parameters to rank the various researched technologies. These weights are based on the several trade studies and are not published in any public documents.

Table 1 Technology Selection Factors with weights

S/N	Parameter	Weight (%)
1	Implementation Cost	8
2	Bandwidth or throughput	22
3	Extensibility	10
4	Size, Weight and Power	10
5	Commercially Available	11
6	Latency	12
7	Open Source/Architecture	12
8	Technical Risk	15
	Total	**100**

Table 2 Selection Factors description with ranking describes the description for each of the selection factors with its ranking weight.

Each technology protocol is weighted against this ranking along with the weights presented in the Table 1 Technology Selection Factors with weights. For each protocol, for each factor a ranking will be assigned and then the ranking is summed. The protocol with the highest number is chosen as the common bus protocol for the proposed common bus network architecture. Protocol analysis is described in the Table2 through Table7. The

Table 8, the Gigabit Ethernet seems to be the best protocol to handle as a common network bus considering all the factors and its weights.

Table 2 Selection Factors description with ranking weight

S/N	Parameter	Description	Ranking Weight
1	Implementation Cost	Hardware & wiring cost.	3 = Low 2= Medium 1 = High
2	Bandwidth or throughput	Maximum bit rate per sec to move data from point A to B	3 = High 2= Medium 1 = Low
3	Extensibility	Complexity of integration of additional devices to the network.	3 = Easy 2 = Moderate 1 = Complex
4	Size, Weight and Power (SWAP)	The hardware size, weight and power consumption.	3 = Lightest 2= Lighter 1 = Light
5	Commercially Available	Easily available commercial hardware.	3= Surplus 2 = Available 1 = Scarcity
6	Latency	The delay in transmitting the data.	3= Low 2 = Medium 1 = High
7	Open Source/Architecture	Publicly available standard protocols and architecture with minimized proprietary standards.	3 = Available 2 = Some proprietary 1 = Proprietary
8	Technical Risk	Technology stability and maturity with no or minimized hardware obsolescence.	3 = Minimum 2 = Medium 1 =High risk.

Table 3 Gigabit Ethernet Analysis

Protocol: Gigabit Ethernet		
Parameter	**Details**	**Ranking**
Implementation Cost	Cheaper COTS products from multiple vendors in terms of routers, switches, cables, and etc.	3
Bandwidth	The bandwidth is 10 Gb/s.	3
Extensibility	Additional devices can be added to the existing network with minimum configuration change	3
SWAP	The network devices are light and consume limited power but we add more devices it creates clutter or cabling issues	2
Commercially Available	A lot of commercially available products from multiple COTS vendors	3
Latency	Depends on the type of networking used. Many hardware has minimum latency compared to other protocols	3
Open Source/Architecture	Standard is available to public no membership	3

	required	
Technology risk	Mature technology since 2002 and is less susceptible to hardware obsolescence.	3

Table 4 CAN bus Analysis

Protocol: CAN Bus		
Parameter	**Details**	**Ranking**
Implementation Cost	Cheaper COTS products from multiple vendors in terms of controllers, connections, and etc.	3
Bandwidth	1MB/sec and multiple devices cannot communicate simultaneously	1
Extensibility	Additional devices can be added to the existing network with minimum configuration change. Not suited for video data transfer. Good for automotive applications.	1
SWAP	The network devices are light and consume limited power	2
Commercially Available	A lot of commercially available products from multiple COTS vendors but no video transferring capabilities.	1
Latency	Minimum latency	3
Open Source/Architecture	Standard is available to public no membership required	3
Technology risk	Mature technology since 1991 and is less susceptible to hardware obsolescence	3

Table 5 IEEE 1394 Analysis

Protocol: IEEE 1394		
Parameter	**Details**	**Ranking**
Implementation Cost	Cheaper COTS products from multiple vendors in terms hubs, cables, and etc.	3
Bandwidth	49MB/s and has a cable length limitation which degrades the performance. Good for video	2
Extensibility	Extensible through hubs but the data transfer rate is low and is not suited for common bus	1
SWAP	The network devices are light and consume limited power but we add more devices it creates clutter or cabling issues	2

Commercially Available	A lot of commercially available products from multiple COTS vendors	3
Latency	The cable length increases latency and is not suited for common bus to handle other types of data than video.	1
Open Source/Architecture	Standard is available to public no membership required	3
Technology risk	Mature technology since 2003 and is less susceptible to hardware obsolescence.	3

Table 6 USB Analysis

Protocol: USB 2.0		
Parameter	**Details**	**Ranking**
Implementation Cost	Cheaper COTS products from multiple vendors in terms hubs, cables, and etc.	3
Bandwidth	60MB/sec and has a cable length limitation which degrades the performance of data.	1
Extensibility	Extensible through hubs but the data transfer rate is low and is not suited for common bus	1
SWAP	The network devices are light and consume limited power but we add more devices it creates clutter or cabling issues	2
Commercially Available	A lot of commercially available products from multiple COTS vendors	3
Latency	The latency increases if more devices connected and the cable length increases.	1
Open Source/Architecture	Standard is available to public no membership required	3
Technology risk	Mature technology since 2000 and is less susceptible to hardware obsolescence.	3

Table 7 DVI Analysis

Protocol: DVI		
Parameter	**Details**	**Ranking**
Implementation Cost	Cheaper COTS products from multiple vendors in terms hubs, cables, and etc.	3
Bandwidth	0.99 GB/s but is not suitable for common bus as this is a serial device and has complex extensibility.	1
Extensibility	Serial interface and cannot be used as a common bus connected other devices	1
SWAP	The network devices are light and consume limited power	3
Commercially Available	A lot of commercially available products from	3

	multiple COTS vendors	
Latency	The cable length increases latency and is not suited for common bus to handle other types of data than video.	1
Open Source/Architecture	Standard is available to public no membership required	3
Technology risk	Mature technology since 1999 and is less susceptible to hardware obsolescence.	3

Table 8 Technology analysis summary

	Ranking with Weight				
Attribute & its weight	**Gigabit Ethernet**	**CAN Bus**	**USB 2.0**	**IEEE 1394**	**DVI**
Implementation Cost (8%)	3* 0.08 = 0.24	3* 0.08 = 0.24	3* 0.08 = 0.24	3* 0.08 = 0.24	3* 0.08 = 0.24
Bandwidth (22%)	3 * 0.22 = 0.66	1 *0.22 = 0.22	1 *0.22 = 0.22	2 *0.22 = 0.44	1*0.22 = 0.22
Extensibility (10%)	3 * 0.10 = 0.30	1 * 0.10 = 0.10	1 * 0.10 = 0.10	1 * 0.10 = 0.10	1 * 0.10 = 0.10
SWAP (10%)	2 * 0.10 = 0.20	2 * 0.10 = 0.20	2 * 0.10 = 0.20	2 * 0.10 = 0.20	3 *0.10 = 0.30
Commercially Available (11%)	3 * 0.11 = 0.33	1 *0.11 = 0.11	3 * 0.11 = 0.33	3 * 0.11 = 0.33	3 * 0.11 = 0.33
Latency (12%)	3 * 0.12 = 0.36	3 * 0.12 = 0.36	1 *0.12 = 0.12	1 *0.12 = 0.12	1 *0.12 = 0.12
Open Source/Arch (12%)	3 * 0.12 = 0.36	3 * 0.12 = 0.36	3 * 0.12 = 0.36	3 * 0.12 = 0.36	3 * 0.12 = 0.36
Technology Risk (15%)	3 * 0.15 = 0.45	3 * 0.15 = 0.45	3 * 0.15 = 0.45	3 * 0.15 = 0.45	3 * 0.15 = 0.45
Total Ranking weight	**2.9**	**2.04**	**2.02**	**2.24**	**2.12**

3.4.2 Bandwidth analysis

The vehicle electronics has to process data real time and has varied bandwidth requirements. At a given point, the bandwidth depends on the type of data it needs to support. In general, they need to process sensor data (including video, image and other mission critical information) and other.

The Table 9 Bandwidth requirement describes the bandwidth requirement for different data types and its frequency (for the proposal purpose, the values in this section are only assumptions). Based on this table, a continuous 3 Gb/s data rate and a frequent 0.37 Gb/s additional data rate is needed always. Keeping the scalability in mind, the 10GB Ethernet bandwidth is chosen for this proposed architecture. All the proposed network devices support gigabit Ethernet. Many sensors and weapon station support gigabit Ethernet. The proposal suggests using gigabit Ethernet supported gateway devices for other non Ethernet based devices.

Table 9 Bandwidth requirement

Data Type	Frequency	Minimum Data rate	Comments
Video	Continuous	0.5Gb/s * 4=2 Gb/s	Assumption: four sensors (cameras) or a computer/storage sending data with a 640 X 480 resolution. The data have to go to storage and display. The compression cannot be revealed here due to security reasons.
Image	Continuous	0.25gb/s *4 = 1Gb/s	Assumption: four sensors (cameras) or a computer/storage sending data with a 640 X 480 resolution. The data have to go to storage and display. The compression cannot be revealed here due to security reasons.
Text data	Frequent	0.02 Gb/se * 5 = 0.1 Gb/s	Assumption: five devices: Data flows between sensors, display, master computer and storage.
Positional data	Frequent	0.12gb/se * 2=0.24Gb/s	Assumption: Two devices; Data flows between sensors, display, master computer and storage.
Mission critical information	Frequent	0.01gb/se * 3=0.03Gb/s	Assumption: Three devices; Data flows from sensors to display.
	Total	**3.37Gb/s**	

3.4.3 Networked devices

The Table 10 lists the proposed networked devices which support 10 GB Gigabit Ethernet bus. All the devices here are assumptions only. The devices and its quantities are just the recommended assumptions are to provide good redundancy, to reduce single point failures, and to reduce size weight and power usage. Some tradeoffs are used to reduce the number of network switches and routers to reduce cost and utilize existing space. The 4 PROPOSED ARCHITECTURE section provides details of the proposed common bus network architecture using these devices.

Table 10 Networked devices with rationale

Device Name	Qty	Rationale
Weapon Station	1	To be lethal. The number varies from vehicle to vehicle
Displays with Controls	4	To be used by the on board crew to execute mission
Sensors	4	To capture and sense data required for mission. Some are

		CAN based and some are Ethernet.
Storage	1	To store information for reuse and other post mission analysis.
Master Computer	2	To provide redundancy and load balance for various mission critical operations.
Gigabit Ethernet (10Gb) Router with minimum 12 ports	2	To provide redundant network connections and to provide dual bus capability and to reduce single point failures. These devices will have built in network management software with some configurations changes.
Gigabit Ethernet Switch(10Gb)	3	To create three different networks and then have a redundant links to reduce single point failures.
CAN to Ethernet Gateway	2	To convert CAN based sensor devices to Ethernet and to provide redundancy and reduce single point failures
USB to Ethernet Gateway	1	To convert USB device display to Ethernet. This is usually for controlling some non mission critical routine tasks. No redundancy is required here as this is non mission critical.
Common Time Module	1	To synchronize common time across network.

3.4.4 Topology selection process

To reduce incidents of single point network failures and increase scalability, a combination of multiple star network topologies is proposed. Every device goes through either a router or a switch. Each device has at least two network paths to reach other devices. The 4 PROPOSED ARCHITECTURE section provides more detailed information about this topology usage in the proposed common bus network architecture.

3.4.5 Alternative architecture proposals

Several alternative proposals were considered to choose an army ground vehicle network architecture. All the architectures were working towards the same basic requirements i.e. reduced single point failures, information assurance (data security), and size, weight & power consumption, and etc. Most of the architectures have the similar organization, but the three candidates were considered as the most valuable architecture proposals to evaluate and choose a best one as the proposed architecture. Three subsections below describe each of the architectures and highlight its advantages and disadvantages. The 3.4.6 Proposed architecture selection process section describes the rationale for selecting the best proposal.

3.4.5.1 Architecture proposal#1

This architecture recommends separate star network for each data classification i.e. classified data will have its own network and unclassified data will have its own network. These separate networks remove any data contamination and complicated software architectures to handle data separation. Each data classification will operate in its own

network and the bandwidth contention is minimal. The Figure 8 shows the architecture proposal#1. This proposes redundant network for each data classification.

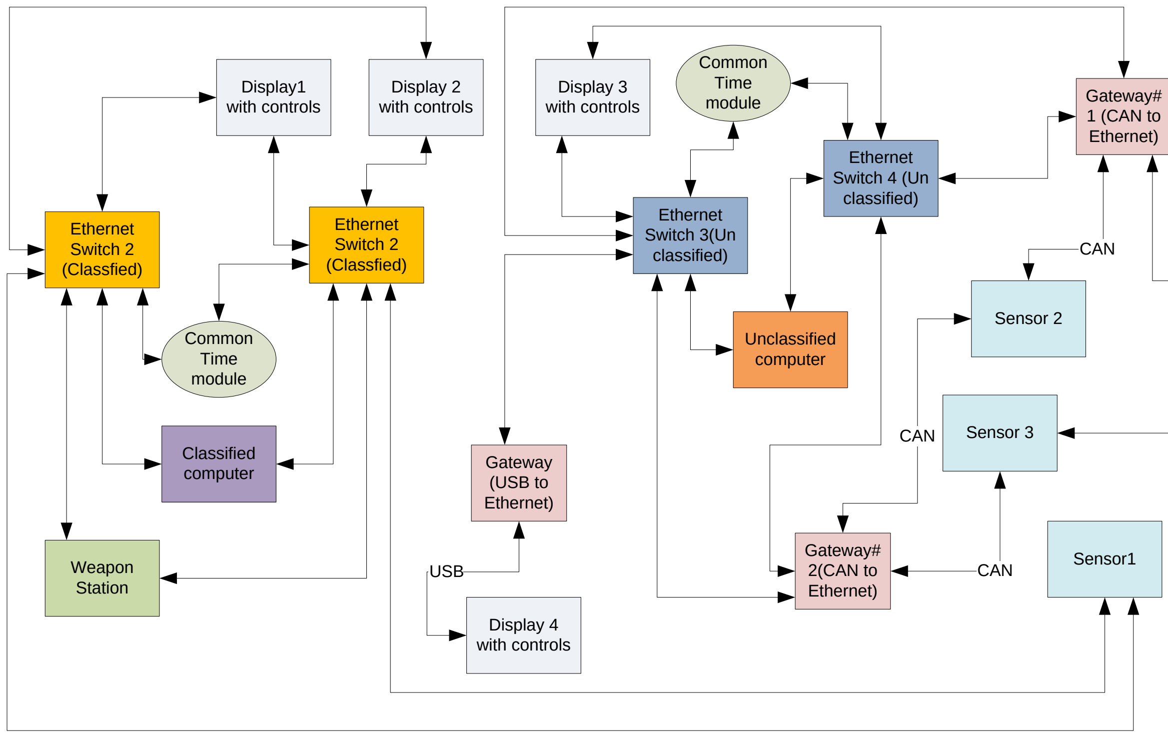

Figure 8 Architecture proposal #1

This architecture proposal#1 has the following high level advantages:

- Common 10GB Ethernet bus to achieve interoperability and extendibility.
- Secure data transmission with no data contamination between multiple data classification (using separate networks per data classification).
- Minimized single point failures with redundancy i.e. every device has at least two paths in the network to reach destination.
- There is no complicated software to handle security (information assurance) due to separate network concept.
- Gateways to achieve protocol conversions.
- Display hardware with embedded software and hardware controls.
- Multiple star network topology using 10GB (Ethernet) bandwidth capable network adaptors and switches.

This architecture proposal#1 has the following high level disadvantages:

- Separate network per data classification (along with redundancy) increases the number of network devices (e.g. secret network, unclassified network, classified

network, and etc.). This creates vehicle clutter and introduces complicated maintenance.

- More devices in the vehicle increases vehicle's size, weight and power consumption issues.

3.4.5.2 Architecture proposal#2

This proposal recommends using10 GB Ethernet bus with a combination of multiple star networks (topology). The architecture also recommends using the combination of both hardware and software solution. The Figure 9 shows the architecture proposal#2. In addition to hardware elements, this architecture proposes four SOA based software components for Data Collection, Data Processing, Data Store, and Data Distribution.

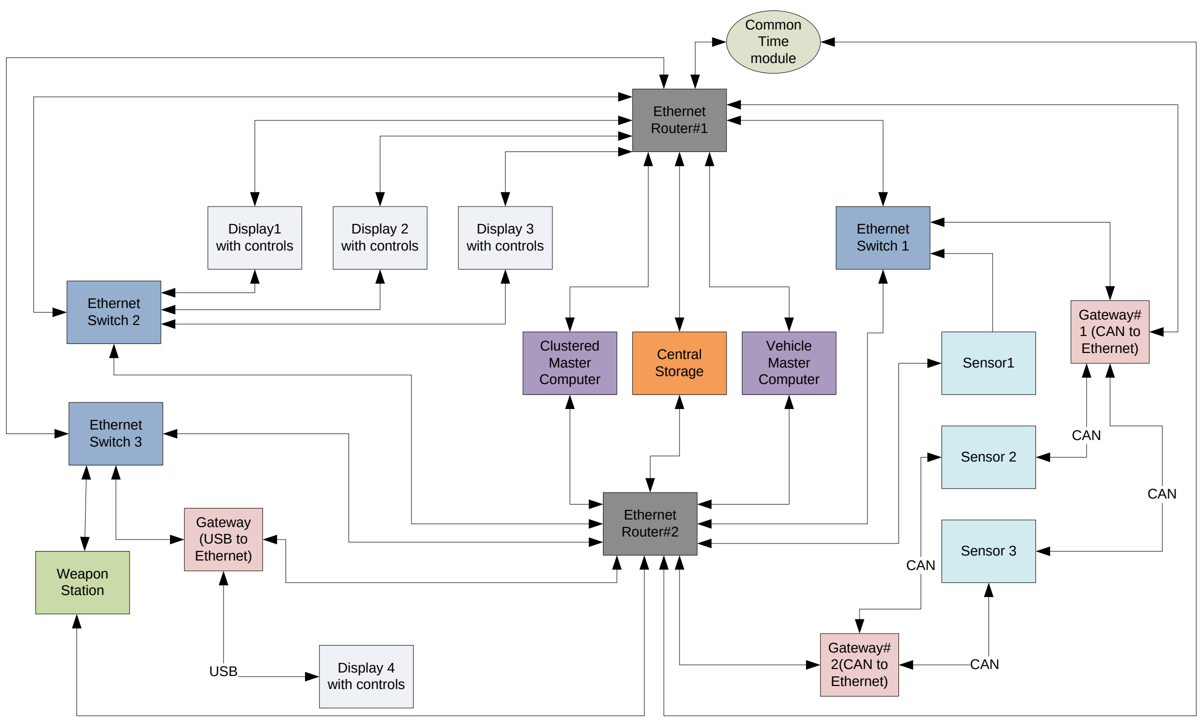

Figure 9 Architecture proposal #2

This architecture proposal#2 has the following high level advantages:

- Common 10GB Ethernet bus to achieve interoperability and extendibility.
- Secure data transmission with no data contamination between multiple data classifications. Classified data access to authorized crew.
- Minimized single point failures with redundancy i.e. every device has at least two paths in the network to reach destination.
- Centralized Service Oriented Architecture (SOA) based software components for data distribution and processing.

- Gateways to achieve protocol conversions.
- Centralized storage and processing devices with load balancing.
- Display hardware with embedded software and hardware controls.
- Minimized size, weight and power requirements.
- Multiple star network topology using 10GB (Ethernet) bandwidth capable network adaptors, routers and switches.
- Built in firewalls in the routers.

This architecture proposal#2 has the following high level disadvantages:

- Requires complex configuration and software models to handle data security and separation of different data classifications.
- If more devices are added, then the existing network switches may not be able to handle them. This requires more switches to the network and it creates size, weight & power consumption issues.

3.4.5.3 Architecture proposal#3

This proposal is a modification of architecture proposal#2 and the focus is on reducing the number of network devices and the wiring. This architecture recommends redundancy at the Ethernet switch level and minimizes size, weight and power consumption issues. The Figure 10 shows the architecture proposal#3.

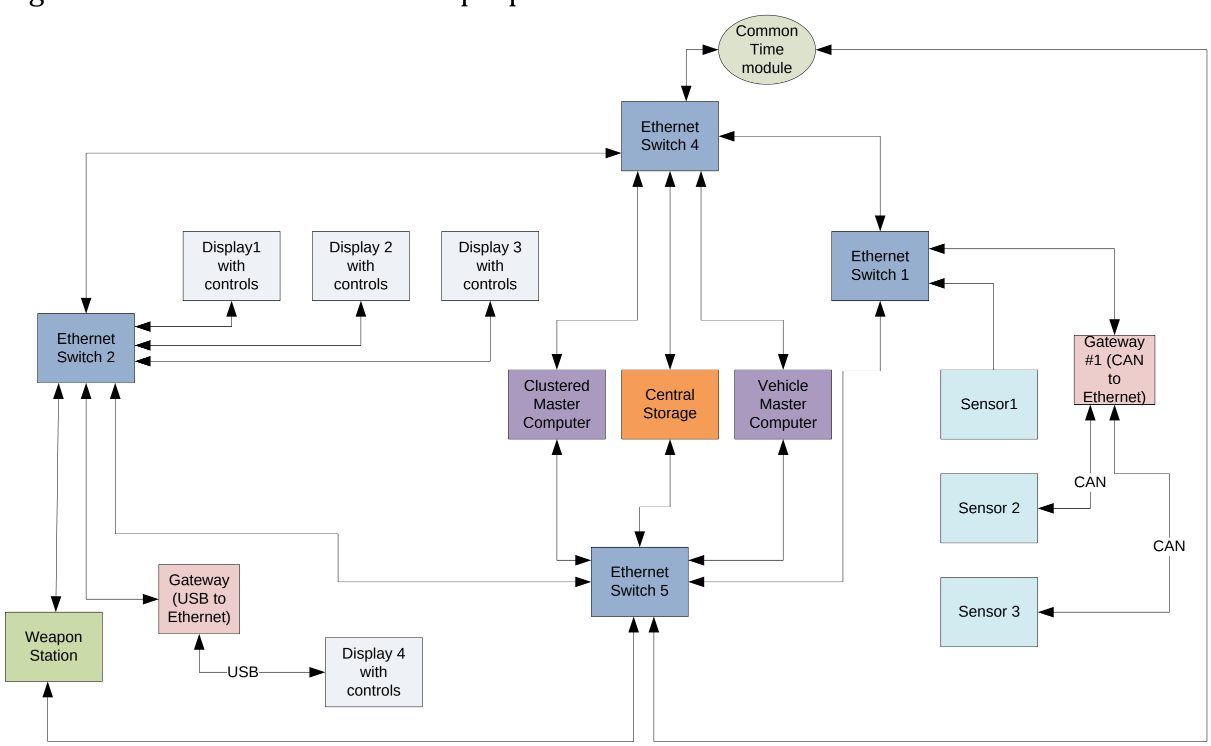

Figure 10 Architecture proposal #3

UNCLASSIFIED: Dist A. Approved for public release

This architecture proposal#3 has the following high level advantages:

- Common 10GB Ethernet bus to achieve interoperability and extendibility.
- Secure data transmission with no data contamination between multiple data classifications.
- Classified data access to authorized crew. This is to conform to the military Information Assurance requirements.
- Redundancy i.e. every Ethernet switch has at least two paths in the network to reach destination.
- Centralized Service Oriented Architecture (SOA) based software components for data distribution and processing.
- Gateways to achieve protocol conversions.
- Centralized storage and processing devices with load balancing.
- Display hardware with embedded software and hardware controls.
- Minimized size, weight and power requirements.
- Multiple star network topology using 10GB (Ethernet) bandwidth capable network adaptors, routers and switches.

This architecture proposal#3 has the following high level disadvantages:

- Display devices have to hop through three switches to reach sensors and it creates latency.
- The redundancy is at the Ethernet switch level and if a device link to the switch is broken, the device will be off the network.
- Requires complex configuration and software models to handle data security and separation of different data classifications.

3.4.6 Proposed architecture selection process

Each of the three proposals are evaluated using the following factors and each factor is given a ranking 1 through 3 (1 is the lowest).

- Data Security (Information Assurance)
- Redundancy
- Single point failures
- Size, weight & power consumption
- Maintenance
- Scalability

Data Security (Information Assurance):

The proposal#1 recommends separate network per data classification and provide highest data security. The proposal#2 and #3 recommend software based highest data security. The proposal#1 sounds best but it requires multiple networks which adds complexity to

the maintenance, size, weight, and power consumption issues. The software based security allows more control with less complexity to maintenance, size, weight, and power consumption. *Per this rationale, the proposal#1 ranks as 2, proposal#2 and #3 ranks as 3*.

Redundancy:
The proposal#1 recommends redundant network per data classification, which creates more number of network devices. The proposal#2 recommends redundant networks and the chances of adding more network devices are slim unless huge number of devices is added to the network. The proposal#3 recommends redundancy at the Ethernet switch level and if a device link to the switch is broken, the device will be off the network.
Per this rationale, the proposal#1 ranks as 2, proposal#2 ranks as 3, and proposal#3 ranks as 1.

Single point failures:
The proposal#1 & #2 recommends redundancy connections at both the Ethernet switch and the device level, which contributes to minimal single point failures. The proposal#3 recommends redundant links at the Ethernet switch level; this contributes to more single point failures for devices. *Per this rationale, the proposal#1 & #2 ranks as 3 and proposal#3 ranks as 1.*

Size, weight & power consumption:
The proposal#1 recommends redundant network per data classification, which creates more number of network devices which contributes to the size, weight & power consumption issues. The proposal#2 proposes redundant networks at both Ethernet switch and device level and does not recommend more switches but it still contributes some size, weight & power consumption issues. The proposal#3 proposes very minimal Ethernet level redundancy and recommends minimal network devices. The proposal #3 contribution of size, weight & power consumption issues are very minimal. *Per this rationale, the proposal#1 ranks as 1, #2 ranks as 2 and proposal#3 ranks as 3.*

Maintenance:
More number of devices and networks per data classification with redundancy make the proposal#1 very hard to maintain. The combination of software based security and redundant networks makes proposal#2 a little hard to maintain. The minimal redundancy with less number of devices in the proposal#3 makes the maintenance a bit easier than other two proposals. *Per this rationale, the proposal#1 ranks as 1, #2 ranks as 2 and proposal#3 ranks as 3.*

Scalability:
The proposal#1 is scalable but it complicates the network, adds too much clutter in the vehicle, and the maintenance is complicated too. The proposal#2 and #3 shares the same levels of scalability issues as proposal#1 but the degree is less due to the software based data security features. *Per this rationale, the proposal#1 ranks as 1, #2 and #3 ranks as 2.*

The table below summarizes the comparison rankings between alternate architectures and influences the best architecture selection from the three evaluated alternative proposals. The proposal with the highest sum of ranking is chosen as the proposed architecture.

Table 11 Architecture comparison

Evaluating Factor	Proposal#1	Proposal#2	Proposal#3
Data Security	2	3	3
Redundancy	2	3	1
Single point failures	3	3	1
Size, weight & power consumption	1	2	3
Maintenance	1	2	3
Scalability	1	2	2
Total	**10**	**15**	**13**

Based on the summary Table 11, the proposal#2 ranked highest with a total of 15 out of 18 ranking points. With this analysis, proposal#2 is considered as proposed common bus network architecture for army ground vehicles. The 4 PROPOSED ARCHITECTURE section describes the architecture in detail.

4 PROPOSED ARCHITECTURE

Army vehicles are used for creating force and moving infantry to battlefield quickly. These vehicles operate in different terrains and electronics in the vehicle continuously monitor and feed mission critical information to crew to carry out their mission.

Each vehicle will have electronic devices and weapons to carry out missions. For an effective operation of these devices, a solid, fault tolerant network architecture is needed. This section proposes a common bus network architecture based on the details provided in the chapters 1 INTRODUCTION through 3 ARCHITECTURE DEVELOPMENT.

4.1 Architecture details with diagrams

The sensors within the vehicle continuously or on demand capture data. The data needs to be displayed, processed, distributed, and stored. The captured data enables crew members to take actions and eliminate enemy forces using on board weapons.

The Figure 11 represents the proposed common bus network architecture for army ground vehicles. The proposed architecture recommends using10 GB Ethernet bus with a combination of multiple star networks (topology). The architecture also recommends using the combination of both hardware and software solution. The proposal is bound to the scope described in the 1.2 Scope section. The additional content in this section describes rationale behind this proposal.

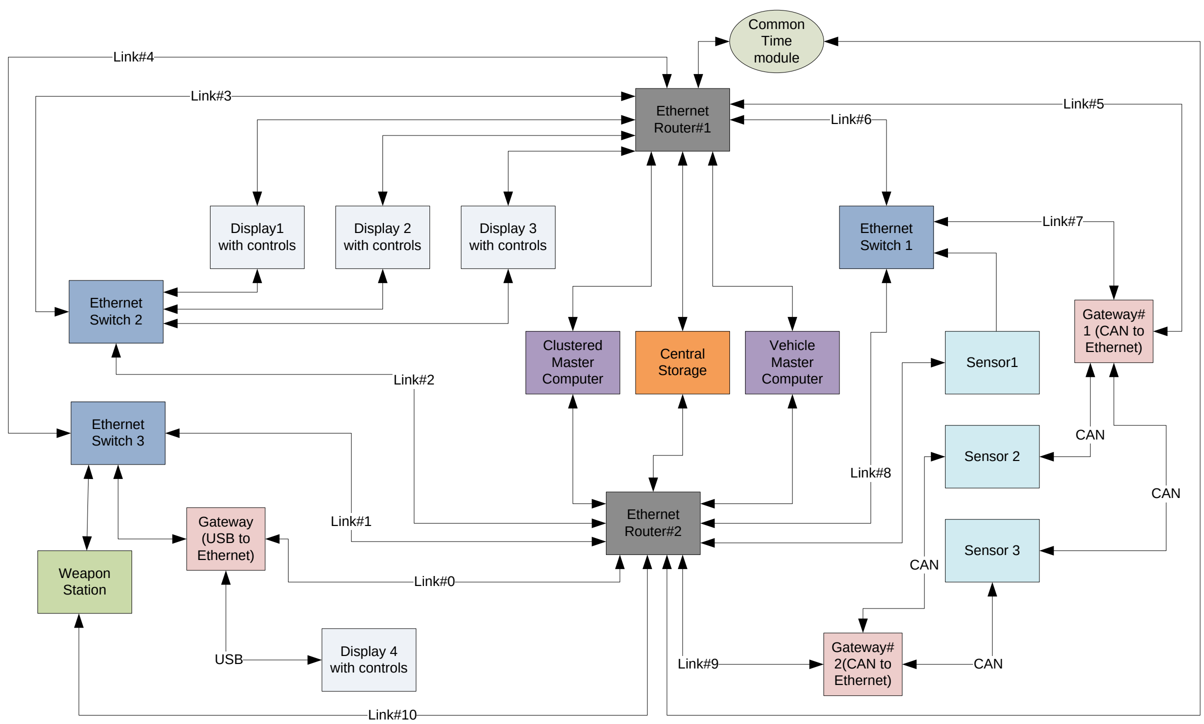

Figure 11 Proposed common bus network architecture

The proposed architecture has the following high level features:

- Common 10GB Ethernet bus to achieve interoperability and extendibility.
- Secure data transmission with no data contamination between multiple data classifications.
- Classified data access to authorized crew. This is to conform to the military Information Assurance requirements.
- Minimized single point failures with redundancy i.e. every device has at least two paths in the network to reach destination.
- Centralized Service Oriented Architecture (SOA) based software components for data distribution and processing.
- Gateways to achieve protocol conversions.
- Centralized storage and processing devices with load balancing.
- Display hardware with embedded software and hardware controls.
- Minimized size, weight and power requirements.

- Multiple star network topology using 10GB (Ethernet) bandwidth capable network adaptors, routers and switches.

For this architecture, the Table 10 provides proposed hardware architecture elements with its rationale. In addition to hardware elements, this architecture proposes four SOA based software components for Data Collection, Data Processing, Data Store, and Data Distribution. This proposal provides only the high level software details and does not provide any low level implementation or code details. The actual software logic details are also not discussed here.

The proposed architecture recommends two 10GB Ethernet router networks with three 10GB Ethernet switched networks for fault tolerance and reduced single point failures.

4.1.1 Sensors networking

The architecture proposes the following to handle sensors in the network. Please refer Figure 11 for the graphic representation.

Physical connection

- Connect all the sensors to Ethernet Switch#1. If a sensor has CAN protocol, use a CAN to Ethernet gateway#1 device to connect to the Ethernet switch#1.
- Connect the gateway device#1 to Ethernet Router#1.
- Connect Ethernet Switch#1 to Ethernet Router#1 and Ethernet Router#2
- To handle redundancy and single point failure, use two CAN to Ethernet gateway devices.
- Connect all the CAN sensors via a gateway#2 to Ethernet Router#2 in addition to connecting to the Ethernet Switch#1.
- Connect Ethernet based sensors to Ethernet Router#2 in addition to connecting to the Ethernet Switch#1.

Rationale:

The proposed physical sensor network allows continuous or on demand data capture. Sensors are connected to two router networks (as described above) which provide high availability and redundancy. They minimize single point failures. Ethernet switch allows easy expansion of additional sensors. If any one network channel is broken, the sensors can be accessed via available redundant network channel. Gateways are used for protocol conversions from CAN. The connection to the routers allows other devices to interact with sensors.

4.1.2 Displays (with controls) networking

The architecture proposes the following to handle displays in the network. Please refer Please refer Figure 11 for the graphic representation.

- Connect all the Ethernet based displays to Ethernet Switch#2.

- Connect all the Ethernet based displays to Ethernet Router#1 in addition to Ethernet Switch#2.
- Connect Ethernet Switch#2 to Ethernet Router#1 and Ethernet Router#2.
- Connect any USB based displays with Ethernet Switch#3 using a USB to Ethernet gateway.
- Connect the USB to Ethernet gateway to Ethernet Router#2 in addition to Ethernet Switch#3.

Rationale:
The proposed physical display devices network allows continuous or on demand data capture from sensors and vehicle master control. Displays are connected to two router networks (as described above) which provide high availability and redundancy. They minimize single point failures. Ethernet switch#2 allows easy expansion of additional display devices. If any one network channel is broken, the displays can access network via available redundant network channel. Gateways are used for protocol conversions from USB. The connection to the routers allows these devices to interact with sensors, weapon station and vehicle master computer.

4.1.3 Weapon station networking

The architecture proposes the following to handle weapon station in the network. Please refer Please refer Figure 11 for the graphic representation.

- Connect Ethernet based weapon station to Ethernet Switch#3 and Ethernet Router#2

Rationale:
Since the weapon station is capable of operating on its own without a networked resource, the weapon station does not have to have too many redundant network channels.

4.1.4 Processing computers and storage networking

The architecture proposes the following to handle processing computers and storage in the network. Please refer Figure 11 for the graphic representation.

- Connect Vehicle master computer, clustered master computer and storage to both Ethernet Router#1 and Ethernet Router#2.
- Connect a common time module (hardware clock with embedded software interface) to Ethernet Router#1 and Ethernet Router#2.

Rationale:
The processing computers are the vehicle's master processing power for functions like data recording, data processing, data distribution, and storage. The storage device provides the media to store the captured data. The physical connection allows these devices to access sensors, displays and weapon stations.

4.1.5 Hardware components

The Table 10 provides the proposed hardware architecture elements and its rationale for using them. The Ethernet routers will have a built in network management software and firewall to control the network. The common time module is connected in the network to allow synchronized time across network.

4.1.6 Software components

The architecture proposes the following software components for data capturing, data processing, data storing and data distributing. All the software components are designed and worked on the Service Oriented Architecture principle. They are developed using high level languages such as C++ or Java. The software components on the display devices provide a user interface designed using human factors engineering. The display devices are the clients and the vehicle master computers are the service providers for the requested data. The display devices will have the capability to interact with any devices in the network with proper access controls.

4.1.6.1 Data capturing

The architecture proposes two types of sensor data capturing mechanisms i.e. batch mode (automatic) and user initiated. The software component is described in high level and it does not provide the low level details (this will be a topic for additional projects).

User initiated capture: Client software resides in all the onboard touch screen supported display devices. The client will be interfacing with the service software installed in the master computer. The client component will have a unique id specific to the display device. Crew members request for sensor data using client software's controls (using touch screen buttons). The client software executes a request for sensor data from the service running on the master computer. The request input will have the user id, password, sensor type, and the unique id. The request will be accepted by the service software and validated. If the requested sensor is a classified data, the service software validates the access authority and then fulfils the request. The requested data will be sent to the display device and then is stored in the central storage for playback later.

Batch (automatic) capture: The service software on the master computer automatically captures all the sensors data continuously and stores in the central storage for later playback.

4.1.6.2 Data processing

The data processing software resides in the vehicle master computer. This performs various processing needed to validate user credentials, encrypt data, and provide processing modules for data distribution and storage. The functions like data compression, data validation, housekeeping, event logging, sensor data recording, executing weapon controls, and etc. This module is invoked when display controls issues appropriate

commands to execute a specific function. This module controls data distribution and data storage software modules.

4.1.6.3 Data distribution

The data distribution software resides in the vehicle master computer. This module takes care of all the controls and algorithms to distribute data between various displays and the sensor devices. This provides mechanisms to distribute data over the wire in a more secure and controlled manner. This module is invoked by the data processing software to delegate data distribution function. The data is distributed over a common Ethernet bus.

4.1.6.4 Data storage

The data storage software resides in the vehicle master computer. This module takes care of all the controls and algorithms to compress and encrypt data, and store data. This provides mechanisms to store data to the central storage in a more secure and controlled manner. This module is invoked by the data processing software. This module encrypts data prior to storing.

4.2 Device performance analysis at faulty conditions

The networks built using this proposed architecture recommends using an alternate path if the primary communication path is faulty or broken. If the primary link is broken, the recommended redundant network layout with high bandwidth (10GB) contributes very minimal performance impact. In this architecture, the network performance degrades only if multiple links are faulty in a given network segment. The main latency in this proposed architecture is due to Ethernet switches, routers and gateway devices.

The bottleneck instances are very minimal in this architecture. This section analyses the device performance when an alternate path is used due to a broken primary paths. For discussion purposes, consider the following three separate instances of faulty primary paths.

- ✓ **Instance1**: Link#2 is broken(refer Figure 11)
- ✓ **Instance2:** Link#5 is broken(refer Figure 11)
- ✓ **Instance3:** Link#10 is broken (refer Figure 11)

For analysis purpose, assume the following:

- One Ethernet switch has a latency of 2 milliseconds at normal loads (Due to store and forward, switch fabric, and queuing latency factors).
- One Ethernet router has a latency of 3 milliseconds at normal loads(Due to routing, security check and jitters)
- One Gateway device has a latency of 2 millisecond at normal loads (Due to protocol conversion and consistency check)

Instance1: *Link#2 is broken (refer Figure 11):*
At normal operation (with no faulty links), the Link#2 in the proposed architecture is used to move data between Display 1-3 & Sensor1. The displays are designed to expect a total of 5 milliseconds latency (from one switch and one router). The Sensor1 is a critical video sensor which transmits video streams at 0.5 GB/s (Refer Table 9) rate and will be used by all the three display (1 – 3) devices. Based on the video content, the user initiates appropriate action e.g. use a weapon station to fire or store the video content to the master computer. In a hostile condition, if the target is moving fast towards the vehicle, the user needs the sensor data at the display device within the expected 5 milliseconds delay.

Assume, the primary link, i.e. Link#2 is broken and the communication has to take the next best path i.e. Link#6. Now, the Ethernet Switch 1 & Ethernet router#1 will have more traffic due to three displays, three sensors and two computers communication. The Link#2 bandwidth has to support the load from all these devices communication. These factors add latency for the Sensor1 data to reach Displays beyond expected 5 milliseconds. If the target is fast approaching and is faster than the delay, the target will hit the vehicle and it may damage the vehicle and crew. At normal load, with this 10GB network bandwidth, contention may not happen but it all depends on the data size being transferred by all the devices concurrently in Link#2.

Instance2: *Link#5 is broken(refer Figure 11):*
At normal operation (with no faulty links), the Link#5 in the proposed architecture is used to move data between Display 1-3 & Sensor2-3. The displays are designed to expect a total of 4 milliseconds latency (from one router & one gateway device). The Sensor2 & Sensor3 sends mission critical information at 0.01 GB/s (Refer Table 9) rate and will be used by all the three display (1 – 3) devices. Based on the content, the user initiates appropriate action e.g. stop the vehicle and check the damage, store the content to the master computer, or relay critical information to the crew members to be alert on a possible mishap. If the critical situation happens and the vehicle is moving fast, the user needs the sensor data at the display device within the expected 4 milliseconds delay.

Assume, the primary link, i.e. Link#5 is broken and the communication has to take the next best path i.e. Link#7+Link6. Now, the Ethernet Switch 1is an extra hop for the data and it contributes 2 more milliseconds of delay. The Sensor2-3 data to reach Displays are now 6 milliseconds than 4. If the critical information is not needed within that time, no problem, else the vehicle and the crew may be in danger (depending on the criticality of the information).

Instance3: *Link#10 is broken (refer Figure 11)*
At normal operation (with no faulty links), the Link#10 + Link#2 in the proposed architecture is used to control weapon station from Display 1or 2 or 3. The weapon station

is designed to expect a total of 5 milliseconds latency (from one switch and one router). Based on the signal sent from the Display device, the weapon station initiates firing. In a hostile condition, if the threat is moving fast towards the vehicle, the weapon needs firing signal from the display device within the expected 5 milliseconds latency.

Assume, the primary link, i.e. Link#10 is broken and the communication has to take the next best path i.e. Link#2+Link#1. Now, the Ethernet Switch 1(in the Link#1) is an added hop for the data and it contributes 2 more milliseconds of delay. The fire signal from the Displays reach the weapon station with 6 milliseconds delay than 4. If the threat is faster than the delay, the target will hit the vehicle and may damage the vehicle and the crew.

4.3 Recommendations & conclusion

This proposed architecture uses standard technologies and promotes open architecture. This architecture does not recommend any vendor specific products and promotes economical procurement. This architecture recommends redundant networks to minimize single point failures. Proposed fast GB Ethernet data buses are faster, scalable and the bandwidth is capable of handling at least five additional sensors and displays. This architecture recommends optimal number of devices on the network to minimize space, power and size allocations. The architecture promotes a common data bus approach and promotes easy expansion. The proposed architecture is scalable and is compliant with the military standards.

This architecture recommends using built in firewalls and network management software on router devices reduces to reduce risks and development costs. The software modules control the data security and distribution between devices.

This proposed architecture can be implemented on any army ground vehicles with minimum modifications. The proposed architecture enables successful battle mission with high availability and faster data transfer. The data is secure and the access is restricted to the authorized personnel. The recommended network technologies are less susceptible to hardware /software obsolescence.

5 FUTURE WORK

This proposed architecture can be extended to the following additional features to enable future work.

- Wireless network architecture with additional security controls in place.
- More software controls and robust software architecture to manage the network and data flow, distribution, and processing.
- Extending to interconnect multiple army vehicles.
- Extending to multiple areas of defense including logistics and maintenance.

- Simulation of this proposed architecture for performance and scalability.

These topics are for multiple projects such as Master's thesis or a Ph.D. dissertation.

REFERENCES

Military Standards

[1.1] "*DoD Architecture Framework Version 1.5"*, "Net centric guidance for architecture product section, April 23, 2007, pp.31 – 37. [Online]. Available: www.defenselink.mil/cio-nii/docs/DoDAF_Volume_II.pdf

[1.2] P. Ross, "Information Assurance (IA) in the Defense Acquisition System," *Department of Defense INSTRUCTION.*, Information Assurance (IA) Implementation, DODI 8500.2, February 6, 2003., pp. 30–35, [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

[1.3] "Multiple Independent Levels of Security/Safety (MILS) ". [Online]. http://www.ois.com/Products/MILS-Technical-Primer.html.[1.4][Online]. http://en.wikipedia.org/wiki/Trusted_Computer_System_Evaluation_Criteria.

Journals

[2.1] S. M. Mahmud, "In-Vehicle Network Architecture for the Next-Generation Vehicles," Chapter XV, *Wayne State University, Detroit*, MI, pp. 281–294. [Online]. Available: http://ece.eng.wayne.edu/~smahmud/PersonalData/PubPapers/IGI-Book-2009.pdf

[2.1] Rabadi, N. M., & Mahmud, S. M. (2007). "Privacy Protection among Drivers in Vehicle-to-Vehicle Communication Networks", Proceedings of the 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, January 11-13, 2007

Articles

[3.1] "System of systems common operating environment (SOSCOE)," Boeing *News, pp. 37-57*. [Online]. http://www.boeing.com/ids/soscoe/120104/SOSCOE_101_New_Rev11-2.swf

[3.2] "In-Vehicle Network design". Saber. [Online]. http://www.synopsys.com/Tools/SLD/MECHATRONICS/Saber/CapsuleModule/saber_invehicle_network_ds.pdf

[3.3] [Online]. http://w3.doshisha.ac.jp/research/research-topics/in-vehicle-network

[3.4] "Service Oriented Network architecture". [Online]. http://www.cisco.com/en/US/netsol/ns629/index.html

[3.5]"Network architecture fundamentals".[Online].
http://www.informit.com/articles/article.aspx?p=21260&rll=1
[3.6]"Controller Area Network (CAN) schedulability analysis: Refuted, revisited and revised" .[Online].http://www.springerlink.com/content/8n32720737877071/
[3.7] "Enterprise Network Design Patterns: High Availability". Sun BluePrints™ OnLine — December 2003. [Online]. http://www.sun.com/blueprints/1203/817-4683.pdf

Books

[4.1] "Network Protocols Handbook by Jawin Technologies", Edition: 2 - 2005, pp-11-32, pp-146-148
[4.2] "Network Security Assessment" by Chris McNab (Oreilly), Edition: 1, March 2004

Wikipedia & other knowledge web sites

[5.1] [Online].http://en.wikipedia.org/wiki/List_of_network_protocols
[5.2][Online].http://en.wikipedia.org/wiki/Network_topologies
[5.3][Online].http://learn-networking.com/network-design/a-guide-to-network-topology
[5.4] [Online].
http://compnetworking.about.com/od/basicnetworkingconcepts/u/computer_networking_basics.htm
[5.5] [Online].
http://www.comptechdoc.org/independent/networking/cert/netmodel.html.
[5.6][Online]. http://www.systec-electronic.com/html/index.pl/en_product_can_ethernet_gateway